THE INTERNATIONAL ORGANISATION OF PENSION SUPERVISORS (IOPS)

DRAFT OECD/ IOPS GOOD PRACTICES FOR PENSION FUNDS' RISK MANAGEMENT SYSTEMS

DRAFT FOR PUBLIC CONSULTATION

DRAFT OECD/ IOPS GOOD PRACTICES FOR PENSION FUNDS' RISK MANAGEMENT SYSTEMS

Introduction

1. Due to the crucial role of private pension systems within the financial markets, and their increasing importance as a source of retirement income for individuals, the effective regulation and supervision of pension funds is becoming ever more important. Yet the regulation and supervision of pension funds are complex issues, not least because pensions are long-term contracts, with a wide social coverage of millions of members and beneficiaries, involving the participation of a range of different players (from pension funds and plans, to financial institutions, plan sponsors and social partners).

2. Pension regulations are increasingly focused on governance and risk management issues. Pension supervisory authorities around the world have also been following other financial sectors and moving towards a risk-based approach to pension supervision. This can be recognized as a structured process aimed at identifying the most critical risks that face each pension fund and, through a focused review by the supervisor, assessing the pension fund's management of those risks and the pension fund's financial vulnerability to potential adverse experience.

3. A key part of a risk-based approach to pension supervision[1] involves the pension supervisory authority transitioning from checking detailed compliance requirements for the operation of pension funds to reviewing the internal decision-making processes and bodies of these funds. One of the main objectives of risk-based supervision is to ensure sound risk management at the institutional level taking into account both the quality of risk management and the accuracy of the risk assessment. Risk-based supervision allows much of the responsibility for risk management to rest with the individual pension fund companies themselves, while the pension supervisory agency verifies the quality of the fund's risk management processes and adapts its supervisory stance in response.

4. Risk management systems can be defined as the process - effected by an organisation's board of directors, management and other personnel - designed to provide reasonable assurance regarding the achievement of objectives in terms of: effectiveness, efficiency and resilience of operations; reliability of financial reporting; and compliance with laws and regulations. The process does not involve just one policy or procedure performed at a certain point of time but should be continually operating at all levels of the organisation, and involve all staff. Internal controls – comprising physical checking mechanisms - are one part of the overall risk system, which also incorporates a holistic philosophy of management oversight, risk awareness, separation of functions, communication, external controls etc.

5. These good practices aim to outline the main features of risk management systems which pension funds employ.[2] They cover the role of management in the risk management process, look in more detail at investment risk, solvency risk and operational risk (including outsourcing) control, and the risk management mechanisms which should be in place (including monitoring and reporting). The good practices also provide guidance for pension fund regulators and supervisors on how to check that such systems are not only in place but are operating effectively.

[1] Introduction to the IOPS Toolkit defines risk-based supervision (reference forthcoming)

[2] The good practices help to complement pension system regulation on integral risk management systems which are implemented in some countries.

Scope and Coverage

6. Despite country-specific situations and supervisory approaches, the OECD and IOPS believe that general good practices on pension funds' risk management can be identified, and will be helpful to members in the supervision of their pension systems. Although these good practices therefore serve as a benchmark reference for all countries or jurisdictions, the question of how to best apply them in practice should take into account country-specific conditions and circumstances. Where the language used in the good practices is directional (such a 'should'), it reflects existing OECD/IOPS recommendations such as already approved principles and guidelines.

7. These good practices are based on the analysis conducted in relation to the OECD/ IOPS Working Paper on risk management[3] and on guidance papers issued by OECD/ IOPS members. The good practices build on the IOPS '*Principles of Private Pension Supervision'*, the OECD '*Guidelines for Pension Fund Governance'*, They also draw on risk management standards in related sectors, such as the Basel Committee for Banking Supervision (BCBS) '*Framework for Internal Control Systems in Banking Organisations'*, the International Association of Insurance Supervisors (IAIS) '*Insurance Core Principles and Methodology*,'[4] and work of the Committee of European Insurance and Occupational Pension Supervisors (CEIOPS).

8. These good practices cover the regulation and supervision of private pensions, including both work-based occupational pensions and personal private pensions.[5] Though mainly referring to pension funds and pension plans,[6] a range of other market participants may be involved (such as plan sponsors or financial institutions serving as external service providers). References to the pension supervisory authority are references to the institution (usually a governmental agency), which is empowered to supervise and oversee the pension sector. It is noted that in some countries this authority is a separate agency, while in many other countries it is integrated with the oversight of other financial activities into a single supervisory body.

---

[3] (IOPS Working Paper No.11/ OECD Pensions and Insurance Working Paper No.40 http://www.iopsweb.org/dataoecd/31/33/43946778.pdf)

[4] Please note that the IAIS ICPs are currently under review with final approval envisaged for 2011.

[5] In EU countries, the good practices may not apply those pension funds and pension plans that fall outside the scope of the EU Directive 2003/41/EC of the European Parliament and of the Council of 3 June 2003 on the activities and supervision of institutions for occupational retirement provision, e.g. pensions funded via book reserves.
Though these good practices apply to private pension funds, it may also be considered good practice to apply similar standards to governmental funds.

[6] According to the OECD's taxonomy, a pension fund is a legally separated pool of assets forming an independent legal entity that is bought with the contributions to a pension plan for the exclusive purpose of financing pension plan benefits. The plan/fund members have a legal or beneficial right or some other contractual claim against the assets of the pension fund. Pension funds take the form of either a special purpose entity with legal capacity (such as a trust, foundation, or corporate entity) or a legally separated fund without legal capacity managed by a dedicated provider (pension fund management company) or other financial institution on behalf of the plan/fund members.

A pension plan is a legally binding contract having an explicit retirement objective (or – in order to satisfy tax-related conditions or contract provisions – the benefits cannot be paid at all or without a significant penalty unless the beneficiary is older than a legally defined retirement age). This contract may be part of a broader employment contract, it may be set forth in the plan rules or documents, or it may be required by law. In addition to having an explicit retirement objective, pension plans may offer additional benefits, such as disability, sickness, and survivors' benefits.

Good Practice 1: Appropriate Mechanisms

1.1 Pension regulatory and supervisory authorities must be satisfied - for licensing/ registration purposes and on an on-going basis - that pension plans and funds have in place a comprehensive risk management system.

1.2 An effective risk management system is comprised of strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report, on a continuous basis, all material risks, at an individual and an aggregated level, to which the pension fund or plan is or could be exposed, and their interdependencies.

1.3 The risk management system needs to be well integrated into the organisational structure and in the decision making process of the pension fund.

1.4 These systems should be commensurate with the size and complexity of the pension fund, reflecting the scope and degree of sophistication of its activities.

Annotations

Risk management systems need to be proportional. For example, larger entities may need committees to help the board with its tasks – such as a risk management, compensation, audit, or compliance committee. The board may alternatively, or in addition, rely on a centralized risk management function, such as a Chief Risk Officer. Whatever the structure chosen, it should reflect the nature of the fund, be established at the commencement of the fund and be clearly articulated.

The following may be considered as the broad categories of risks which pension funds face.[7] It should be noted that not all risks apply to each type of fund, and any risk management system needs to identify which risks are material to the particular fund in question (according to whether it is a defined benefit or defined contribution fund, offers guarantees, is funded by a plan sponsor etc.).

- *Investment or market risk*: risk of losses due to adverse movements in interest rates and other market prices. The risk may also arise due to investment in unregulated/ unlisted products. 'Concentration' risk is also possible – i.e. risk that the pension fund's portfolio is not adequately diversified and is too exposed to one asset or issuer.

- *Counterparty default risk / credit risk*: risk of loss from the failures of a counterparty to meet its obligations.

- *Funding and solvency risk*: the risk that a pension fund does not have sufficient assets to meet its liabilities.

[7] The IOPS Toolkit for Risk-based Supervision contains further details.

- *Liquidity Risk:* the risk that an institution will not be able to meet its payment obligations as they fall due.

- *Asset-Liability mismatch risks:* risk arising from insufficient assets to meet liabilities, which may arise from, for example, adverse market movements having a differential effect on assets and liabilities.

- *Actuarial risk*: risk arising from inappropriate actuarial valuation methods and assumptions (e.g. mortality, longevity, disability, inflation, liquidity etc.)

- *Agency risks*: risks which could otherwise be described as 'competition risk' or 'competition failure'. Issues include excessive fees, conflicts of interest, biased funding decisions, fraud misappropriation and misallocation.

- *Operational and outsourcing risks:* the risk of losses resulting from inadequate internal processes, people and systems, including IT systems, as well as the risks related to the outsourcing of business activities. Recording keeping risks (such as errors in investment holdings, benefits not paid or late contributions etc.) would also be included. IT risk - a subset of operational risk - is the risk arising from inadequate information technology and processing in terms of manageability, exclusivity, integrity, infrastructure, controllability and continuity.

- *External and strategic risk:* these are the inherent risks with regard to the sensitivity of the fund to external factors (such as political risk, demographics, competition, technology, reinsurance, mergers, plan sponsor risk, political stability, natural disasters, etc.). The risk of non-payment of contributions should also be considered.

- *Legal and regulatory risk:* the likelihood of adverse consequences arising from the failure to comply with all relevant laws and regulations.

- *Contagion and related party/ integrity risk:* risks arising as a result of close association with another entity – the risks may be direct through financial exposure or indirect through reputation damage.

Good Practice 2: Management Oversight and Culture

2.1 The governing board of the pension fund or plan[8] should be responsible for defining, implementing and improving the pension fund or plan's risk management system, and for establishing a highly ethical standard throughout the organisation.

2.2 The governing board of a pension fund or plan should approve and regularly review its overall risk management strategy. This process involves understanding the risks run; setting acceptable levels of risk; and outlining how these risks will be measured monitored and controlled

2.3 In order for risk assessment to remain effective, the governing board needs to frequently evaluate the risks affecting the achievement of its goals and react to changing circumstances and conditions.

2.4 As well as setting up the risk management system, the governing body shouldcheck that it is working effectively on an on-going basis and that there is a process in place for modifying or adapting the strategy as required.

2.5 The risk management strategy needs to be documented, communicated to all relevant staff members and followed.

2.6 There should be a clear division of responsibilities within the organisation. Decision making, execution and checking functions should be assigned to different people and have suitable oversight. The division of responsibilities should reflect the nature and extent of the risks posed.

2.7 It is the responsibility of the governing board to develop a strong internal control culture within its organisation, a central feature of which is the establishment of systems for adequate communication of information between levels of management.

2.8 A conflicts of interest policy (including disclosure and review procedures) and a code of conduct policy for all staff should also be in place.

2.9 Policies and practices (including compensation) that may inadvertently provide incentives or temptations for inappropriate activities should be avoided

Annotations

Management oversight and a control culture are a vital part of a functioning risk management system.

Risk management strategies cover all material risk, including operational risks. An effective risk assessment will normally seek to identify and consider internal factors (such as the complexity of the organisation's structure, the quality of personnel, organisational changes and employee turnover) as well

[8] In a two-tier board system, involving a managing board and a supervisory board, the body which is responsible for all strategic decisions (usually the managing board) is considered the governing board.

as external factors (such as fluctuating economic conditions or technological advances) that could adversely affect the achievement of the pension fund's goals.

There are both measurable and non-measurable aspects of risks, and the risk management strategy needs to weigh the costs of controls against the benefits they provide. Risks will have to be evaluated to determine which are controllable and those which are not and whether the former should be accepted or managed, and how both can be mitigated.

In order to document the risk management strategy, a 'risk register' may be used, including an assessment of the implications of risks identified and solutions for managing risk.

As the ultimate body responsible for the operation of the pension fund, the governing board would be expected to periodically discuss the effectiveness of the risk management system. This requires reporting systems and internal control that allow the board to receive unfiltered, accurate information.

Risk management systems will typically include an organizational chart (showing who is empowered to sign for the fund and who is empowered to approve decisions etc.), and a written manual (describing the division of tasks, responsibilities, powers). The strict separation of incompatible functions is an important way to avoid conflicts of interest.

For smaller organisations with limited numbers of staff, it may be difficult to assign clear division of responsibilities and powers. However, there is still a need for transparent mechanisms for handling conflicts of interest, particularly as smaller organizations tend to outsource key functions and may rely more heavily on key external advisors.

Instilling a risk management culture in a pension fund as a whole must come from the top, with the board leading by example. This ensures that risk management is not a 'box ticking' exercise, but is truly embedded in the operations of the organisation.

An essential element of a strong risk management system is the recognition by all employees of the need to carry out their responsibilities effectively and to promptly communicate to the appropriate level of management any problems in operations, instances of non-compliance with the code of conduct, or other policy violations or illegal actions that are noticed. In cases of non-compliance, policy violations or illegal problems which are materially significant to the plan, there may be the need to whistle blow this to the pension supervisory authority.

Competent employees may be secured by appropriate recruitment, ongoing training, setting motivational targets, incentive driven career paths etc. Individual mobility and transfer of responsibility at all levels may guard against problems which can arise out of routine/ habit.

Conflicts may arise whenever the decisions of a board member or management concerning the pension fund are, or may be perceived to be, affected by a separate personal interest or a duty owed to another party, rather than that of the pension plan/ fund members and beneficiaries.

A policy for handling conflicts of interest would normally include the following three stages: ***identification*** (i.e. understanding – via training if necessary – of what could constitute a conflict and notification of any outstanding***); monitoring*** (via an up-to-date register of interests –e.g. financial

interests and other appointments, role of third parties and fees paid – and recording how they are managed via minutes of meetings); ***managing*** (according to the nature of scale of the conflict).

Some conflicts may be managed – such as by outlining prohibited transactions, restricting outside personal appointments, using subcommittees, appointing an independent chair, conflicted members abstaining from debates or votes, disclosure. Others may be so acute that they are best avoided entirely – for example through the resignation of the conflicted member and appointment of an independent board member, or require further legal advice.

The internal code of conduct for the staff of the institution would generally include broad principles of conduct among them: integrity, objectivity, accountability, openness, etc. Such codes normally cover subjects such as ethical behaviour, declaration of gifts, complaints procedures, use of confidential information, etc.

Policies and practices that may inadvertently provide incentives or temptations for inappropriate activities include undue emphasis on performance targets or other operational results, particularly short-term ones that ignore longer-term risks; compensation schemes that overly depend on short-term performance; ineffective segregation of duties or other controls that could allow the misuse of resources or concealment of poor performance; and insignificant or overly onerous penalties for improper behaviour.

Appropriate compensation can provide the right incentives for good performance. A compensation committee may optimize the process of evaluating the compensation of those responsible for the operation and oversight of the pension fund, such as asset managers, custodians, actuaries, as well as the members of the governing board. The compensation of sales forces of pension plan providers may warrant particularly close scrutiny.

Good Practice 3: Funding and Solvency Risk Control

3.1 Pension funds that offer defined benefits or guarantees need to maintain an appropriate level of assets to meet the liabilities corresponding to the financial commitments or obligations which arise out of the pension arrangement.[9] Such pension funds should be required to establish a funding and solvency policy.

3.2 The funding and solvency policy should be consistent with legal provisions (funding and benefit security regulations), setting out the mechanisms for monitoring the funding level and identifying the main funding and solvency risks to be monitored.

3.3 At a minimum, the policy would normally also lay out the valuation methods for calculating the funding level (the ratio of assets to liabilities), the target funding level, the amortisation or recovery period for meeting situations of underfunding and the means through which funding gaps will be closed,

[9] See *OECD Guidelines on Funding and Benefit Security in Occupational Pension Plans* for further details http://www.oecd.org/dataoecd/3/22/38547978.pdf

and the procedures to be followed to address a situation of overfunding, both on an ongoing basis and if the plan is terminated or the fund liquidated.

3.4 This policy also needs to establish a procedure to collect late contributions from the sponsoring employer or/and plan/ fund members, including judicial procedures where relevant.

3.5. The funding and solvency policy should be reviewed regularly by the board, and at least every three years.

Annotations

When laying out its funding and solvency policy, the governing board may need to consider the following issues:

- the nature of the benefit promise, and in particular, the extent to which accrued and future benefits, retirement ages and other plan parameters affecting pension benefits may be altered;
- the sources of financing for the pension fund, including an assessment of the financial strength of the plan sponsor,
- the extent to which the fund itself – or its managing entity - is responsible for any guarantees;
- the presence of external forms of solvency and benefit protection, such as insolvency guaranty arrangements which protect benefits against the bankruptcy of the pension fund, its managing entity or the plan sponsor.

A key component of this policy is the procedure to be followed in case of underfunding. There may be different mechanisms permitted for correcting underfunding, such as the payment of a lump sum or contingent financial commitments by the plan sponsor, an increase in future contributions by the sponsor or/and plan / fund members, and adjustments in future benefit accruals and other benefit parameters such as the retirement age.

When monitoring the funding level of the pension fund, the board will normally rely on the advice of an actuary. Such monitoring would normally include a spot check on the current funding level (as required by the legal provisions), but also stochastic and scenario or stress-testing to assess the fund's resilience to withstand major shocks in the future (including mortality and longevity risk).

Good Practice 4: Investment / Market Risk Control

4.1 A written investment policy should be required to manage investment risk.[10] The investment policy should be consistent with legal provisions (prudent person and quantitative limits) and the objectives of the fund (i.e. with the characteristics of the liabilities, maturity of obligations, liquidity needs, risk tolerance etc,), at a minimum identifying strategic asset allocations (i.e. the long-term asset mix over the main investment categories), the performance objectives (and how these will be monitored and modified), any broad decisions regarding tactical asset allocation, security selection and trade execution. A socially responsible investment policy may also be added to the overall investment strategy, outlining how the pension fund intends to consider and manage environmental, social and governance risks.

4.2 The investment policy also needs to address the use of internal or external investment managers (with an investment management agreement required for the latter), and establish mechanisms for monitoring the costs of such services.

4.3 The investment policy for pension plans in which members make investment choices should ensure that an appropriate array of investment options, including a default option, are provided for members and that members have access to the information necessary to make investment decisions, and the investment policy should classify the investment options according to the investment risk that members bear.

4.4 The investment policy should stress that pension funds should only invest in assets and instruments whose risk the pension fund concerned can properly monitor, manage and control.[11]

4.5 Given the specific nature and complexity of some financial instruments (in particular, derivatives and alternative investments such as hedge funds and private equity), the investment policy should specifically address how the underlying risks of these instruments will be monitored and managed.

4.5 The written investment policy should be reviewed regularly by the board, and at least every three years.

Annotations

At the heart of the risk management system of any pension fund or plan is the investment strategy – investment, counterparty and liquidity risks being major challenges for any fund.

A comprehensive investment policy would normally contain the following elements:

[10] See *OECD Guidelines on Pension Fund Asset Management* for further details http://www.oecd.org/dataoecd/59/53/36316399.pdf

[11] See IOPS '*Good Practices in Risk Management of Alternative Investments by Pension Funds'* for further details http://www.iopsweb.org/dataoecd/47/20/40010212.pdf?contentId=40010213

- Investment objectives
- Asset allocation
- Diversification
- Liquidity need
- Valuation methodology
- Use and monitoring of derivatives
- Asset Liability Matching targets (where appropriate)
- Performance measurement, monitoring and benchmarking
- Control procedures, including risk tolerances / risk monitoring procedures
- Reporting format and frequency
- Investment in alternative assets
- Leverage of fund (where appropriate)

Investment in certain asset classes calls for special risk controls. For instance, alternative investments require an assessment of the extent to which they fit with the pension fund's overall strategy, diversification objective and risk profile. Pension funds and plans need to have a clear understanding of the risk characteristics of any alternative investments (which require regular checking). They need to have confidence in the managers of any funds they invest in, and pay particular attention to reports and valuations from fund of funds. Contract terms (lock up periods etc.) also require checking, and particular attention given to valuation policies of unlisted assets during volatile market conditions. Consideration also needs to be given to liquidity management in relation to infrastructure or other private asset investments.

A key driver of the asset strategy adopted by pension funds offering defined benefits or guarantees will be its liabilities profile, and the need to ensure that it holds sufficient assets of appropriate nature, term, liquidity to enable it to meet those liabilities as they become due. Detailed analysis and management of this asset/ liability relationship will therefore be a pre-requisite to the development and review of investment policies and procedures which seek to ensure that the pension fund adequately manages the investment-related risks to its solvency. The analysis will involve, inter alia, the testing of the resilience of the asset portfolio to a range of market scenarios and investment conditions, and the impact on the pension funds' solvency position.

Given the investment strategies of DC plans may involve specific risks specific internal controls may be required. For example, as many members invest in the plan's default fund, this would need to be reviewed carefully.

Good Practice 5: Operational and Outsourcing Risk Control

5.1 An operational risk management system should be drawn up, identifying a set of procedures, which include procedures to define, identify, assess, monitor and control operational risk. This will cover IT risks and include a business continuity plan.

5.2 The pension fund needs to develop a written policy regarding outsourcing which should be approved by the governing board and senior management. The policy needs to be regularly assessed and updated with any necessary changes implemented.

5.3 Where an outsourcing agreement has been entered into, although the business activity or function is delegated, the governing board of the pension fund remains accountable for the outsourced business activity.

5.4 To manage the risk of outsourcing activities, the governing board of the pension fund needs to check that their service providers have set up appropriate control systems before appointing them. This will be part of a due diligence, tender process and include signing a written outsourcing agreement.

5.5 Service providers need to be monitored on an on-going basis, with the outsourcing agreement containing clear service requirements and details of how, and how frequently, these will be measured. The governing board of the pension fund may require access to information and the premise of the service provider (themselves or via an audit) to check that the conditions of their agreement are being met.

5.6 Conditions for how the agreement can be terminated, and continuity/ hand-over provisions also need to be laid out.

Annotations

Operational risk is the risk resulting from inadequate or failed internal processes, people and systems or from external events. Such risks include administrative errors (for example arising from the wrongful assignment of contributions), IT errors or failures (leading to data loss or trading mistakes), as well as the more serious risk of fraud and external risks such as contagion from related parties facing financial difficulties, political instability, natural disasters (such as damage to buildings due to fire, floods or earthquakes) and crime (burglary or theft of fund property).

Models which attempt to quantify the level of future operational risk could be developed. Quantification can be used to assess the efficiency of the fund in controlling risks and/or in providing an estimation of the capital required to absorb potential losses from operational risk events.

With all types of financial services now highly dependent on technology, internal controls are needed to verify the security of the IT systems. IT risks include risks of error, fraud, negligence, and chance mishaps (such as system crashes), the concentration of data, which can weaken the security of information and the use of complex applications which can result in the repetition of problems. Controls are needed to ensure the physical and logistical security of data, including the protection of files and software. The information processes, operational software systems, and accounting and financial reporting systems should be regularly reviewed. Contingency plans using an alternate off-site facility, including the recovery of critical systems supported by an external service provider, are also required.

Controls over information systems and technology would normally include both general and application controls. General controls are controls over computer systems (for example, mainframe, client/server, and end-user workstations) and ensure their continued, proper operation. Application controls are computerised steps within software applications and other manual procedures that control the processing of transactions and business activities, including, for example, edit checks and specific logical access controls unique to a business system. Necessary protection measures will include: IT security requirements (data protection, firewalls); data backup; system recovery; password controls (including a password policy addressing password strength and complexity etc.). Monitoring and incident management controls are also essential.

In addition to the risks and controls above, inherent risks exist that are associated with the loss or extended disruption of services caused by factors beyond the organisation's control – hence the need for contingency plans. Business resumption plans must be periodically tested to ensure the plan's functionality in the event of an unexpected disaster.

The risk from pension funds outsourcing activities needs particular attention. The quality of the internal control systems of pension fund service providers may pose a threat to the funds and thus the interests of plan / fund members and beneficiaries. The oversight of these service providers should therefore be part of the pension fund's own risk management system.[12]

An outsourcing agreement is an arrangement between the governing board of a pension fund and a service provider for the performance of a business activity of the pension fund. A material business activity is one which has the potential, if disrupted or poorly performed, to affect members' or beneficiaries' interests, or to have a significant impact on the business operations, reputation, rate of return, profitability or net assets of a pension fund. The outsourcing policy would normally contain considerations of the impact of outsourcing on its business and the reporting and monitoring arrangements to be implemented once outsourcing is undertaken. When considering whether to outsource an activity, the pension fund's governing board would normally assess whether the business activity is material, the cost of the outsourcing arrangement, and the degree of difficult (including time taken) to find an alternative service provider or to bring the service in-house.

[12] Information on management of outsourcing risk drawn from Australian Prudential Regulation Authority guidance, as well as CEIOPS and BCBS good practices.

Due diligence for the evaluation and selection of a service provider involves at a minimum assessing the financial and technical abilities, system and capabilities of the service provider to deliver the required services and an assessment of the service provider's internal control system – including performance standards, policies, procedures, compliance, reporting and monitoring processes. A tender process could be considered as a good practice component of the due diligence process. All due diligence should be suitably documented.

Signed, written outsourcing agreements will include details of any default arrangements, a dispute resolution process, liability and indemnity provisions, confidentiality requirements, and details of pricing and fee structures.

Audit, monitoring and assessment procedures - specifying service levels and performance requirements – need to be clearly laid out. The frequency of reporting against targets should reflect the level of risk to the fund in event of the failure of the service provider to perform at a certain level. The agreement needs to provide the governing board of the pension fund and the pension supervisory authority (where appropriate)[13] with access to information, including access to the service providers' premises, and the right of the governing board or pension supervisory authority to require an audit. Service providers may not charge a fee for such information or access.

Termination provisions need to be transparent and clear to all parties, and business continuity planning included.

Good Practice 6: Control and Monitoring Mechanisms

6.1 Control mechanisms – both internal and external - operate at every level and are an integral part of daily activities, at the top management level, as well as within each department. They normally comprise of physical controls and checking for compliance with exposure limits, as well as systems for verification and reconciliation etc.

6.2 Monitoring needs to be part of daily activities but also include separate periodic evaluations of the overall internal control process, with the frequency of monitoring different activities determined by the risks involved and the frequency and nature of changes occurring in the operating environment.

6.3 Adequate monitoring systems should be in place. Risk management systems need to ensure that transactions have been carried out by the persons assigned, in ways authorized by the managing board (delegation of signatures, division of tasks and control procedures etc.). Decision making (or authorizing decisions), protection of assets, accounting and control need to be assigned to different staff members.

[13] Alternatively the pension supervisory authority should have mechanisms in place to liaise with the appropriate financial sector oversight body.

6.4 Key elements of the risk management and monitoring system are the internal audit and compliance functions – the nature and scope of which should be appropriate to the operations of the pension fund. These functions report directly to the governing board and they should not conflict with other obligations. Those responsible for internal audit and compliance require access records and communicate freely to carry out their role effectively.

6.5 Performance measurement and compensation mechanisms should be part of risk management systems. The performance of the persons and entities involved in the operation and oversight of the pension fund should be assessed regularly, particularly where the governing board of the pension fund or plan is also a commercial institution.

6.6. In addition to – and working with – the internal control mechanisms, independent external parties should be appointed as part of the risk management of a pension system. Third parties such as external auditors, actuaries and custodians should be independent and have 'whistle blowing' responsibilities.[14]

Annotations

Monitoring evaluations can be done by personnel form several different areas, including the business function itself, financial control and internal audit. Separate evaluations of the internal control system often take the form of self-assessments when persons responsible for a particular function determine the effectiveness of controls for their activities. The documentation and the results of the evaluations are then reviewed by senior management. All levels of review need to be adequately documented and reported on a timely basis to the appropriate level of management – with the governing board having ultimate oversight. Monitoring mechanisms will include senior management clarifying which personnel are responsible for which monitoring functions.

The internal auditing function within a pension fund should cover the effectivness of operations, the reliability of financial reporting, deterring and investigating fraud, safeguarding assets, and compliance with laws and regulations.

Performance of the compliance function may be delegated by internal audit to a separate area, depending on the size and complexity of the pension fund, among other factors. The compliance function advises management on compliance with laws and regulations and may also produce assessments of the possible impact of any significant changes in the legal environment on the operations of the undertaking concerned the identification and assessment of compliance risk.
The compliance function, along with the internal audit must have unrestricted access to all departments and information; be suitably independent (reporting to the board); have sufficient weight and resources to carry out its task. In terms of good practice, the reports of the compliance function and internal audit will be issued directly to the governing board of the pension fund or plan or its audit committee, and to senior management, thereby providing unbiased information about operational activities. Due to the important nature of their tasks, the compliance function and internal audit must be staffed with competent, well trained individuals who have a clear understanding of their role and responsibilities.

[14] See also OECD '*Guidelines for Pension Fund Governance'*.

Responsibilities of the internal audit include ensuring compliance with all applicable policies and procedures and reviewing whether the fund's policies, practices and controls remain sufficient and appropriate.

Further independence of the internal audit function can be reinforced by the governing board of the pension fund or plan having such matters as the compensation or budgeted resources of the internal audit determined by the board or the highest levels of management rather than by managers who are affected by the work of the internal auditors.

Mechanisms are needed to assess regularly the performance of the pension fund's internal staff, as well as external service providers (e.g. those providing consultancy, actuarial analysis, asset management, custody another services). Objective performance measures should be established for all the persons and entities involved in the administration of the pension fund. For example, appropriate benchmarks should be established for external asset managers. Performance needs to be regularly evaluated against the performance measures and results should be reported to the relevant decision maker, and, where appropriate, to the supervisory board, the pension supervisory authority, and the pension plan/ fund members and beneficiaries. The benchmarks need to be reviewed regularly also to ensure their consistency with the pension fund objectives (e.g. the investment strategy).

Internal controls need to be revised to appropriately address any new or previously uncontrolled risks (e.g. from financial innovation, such as new asset allocation strategies and alternative investments). External control mechanisms include:

- Reports from the supervisory board
- Use of separate custodian
- Actuarial reports
- External Audit

External auditors have an important impact on the quality of risk management through their audit activities. They have particular responsibility for assessing the management of solvency risk, for example through checking longevity and other actuarial assumptions used by the fund to estimate their liabilities. External auditors can influence risk management systems in various ways, including through discussions with management and recommendations for improvement, which provide important feedback on the effectiveness of the internal control system. External auditors have to obtain an understanding of the internal control system in order to assess the extent to which they can rely on the system in determining the nature, timing and scope of their own audit procedures.

Though the nature and extent of the external audit will vary by country, it is generally expected that material weaknesses identified by the auditors would be reported to management in confidential management letters and, in many countries, to the pension supervisory authority, and that external auditors may be subject to special supervisory requirements that specify the way that they evaluate and report on internal controls.

Good Practice 7: Information, Reporting and Communication

7.1 Adequate and comprehensive channels for the reporting and communication of internal data, external information (e.g. from service providers and to pension supervisory authorities) and external market information (in particular to plan /fund members)[15] should be established, with all information required to be reliable, timely, accessible and consistent. A policy should also be in place to ensure that confidential information is treated appropriately.

7.2 Efficient reporting is an important part of any risk management system. Information needs to be released to the necessary parties in an understandable format, and with due frequency. Separate records should be kept for each pension fund or account.

7.3 Effective channels of communication are required so that everyone understands their responsibilities and to make sure that relevant information is reaching the appropriate personnel. Communication lines should encourage adverse reporting (whistle blowing) – particularly when flowing upwards.

7.4 Internal control deficiencies, or ineffectively controlled risks, should be reported to the appropriate person(s) as soon as they are identified, with serious matters reported to senior management and the board of directors

Annotations

Effective information flows are vital for risk management systems to operate properly. Information is enhanced by effective communication. The organisational structure needs to facilitate an adequate flow of information - upward, downward and across the organisation. A structure that facilitates this flow ensures that information flows upward so that the board of directors and senior management are aware of the business risks and the operating performance.

Information flowing down through an organisation ensures that objectives, strategies, and expectations, as well as its established policies and procedures, are communicated to lower level management and operations personnel. Communication across the organisation is necessary to ensure that information that one division or department knows can be shared with other affected divisions or department.

Appropriate reporting mechanisms also need to be in place for receiving information from external service providers.

Appropriate reporting mechanisms to the pension supervisory authority are also required (reporting activities on an on-going, regular basis, not only performance numbers). Such reporting should include notifying the pension supervisory authority, in a timely manner, prior to the outsourcing of critical or important functions as well as of any subsequent material developments with respect to those activities (e.g. a change in service provider, a major problem with the performance of a service provider etc.).

[15] See *OECD Guidelines for the Protection of Rights of Members and Beneficiaries in Occupational Pension Plans* *http://www.oecd.org/dataoecd/16/33/34018295.pdf*

Once reported, it is important that management corrects deficiencies on a timely basis. The internal auditors need to conduct follow-up reviews or other appropriate forms of monitoring, and immediately inform senior management or the board of any uncorrected deficiencies. In order to ensure that all deficiencies are addressed in a timely manner, senior management are responsible for establishing a system to track internal control weaknesses and actions taken to rectify them.

Good Practice 8: Supervisory Oversight of Pension Funds' Risk Management Systems

8.1 The regulatory or supervisory authority should have the power to evaluate the directors and governing boards of pension plans, and to determine that appropriate corporate governance, risk management and internal controls and a code of conduct will be in place (appropriate meaning reflecting the scope and degree of sophistication of the proposed activities of the applicant).[16]

8.2 Pension supervisory authorities can indicate the type of risk management systems they expect pension funds and plans to have in place either through regulatory requirements or through issuing guidance (or even, where appropriate, by providing training).

8.3 An evaluation of a pension fund or plan's risk management system should be central to on-going supervisory assessment as well as part of any licensing or registration criteria. The supervision of risk management systems should be proportional to the size and complexity of the pension fund.

8.4 In those instances where supervisors determine that the risk management system is not adequate or effective for the organisation's specific risk profile, they should take appropriate action. This would involve communicating their concerns to senior management and monitoring what action is taken to improve risk management .

8.5 Pension fund supervisory authorities should aim to adopt a risk-based approach in their supervision of risk management systems.[17]

8.6 Pension supervisory authorities should where possible directly monitor the risk management systems of the service providers which perform important outsourced functions for pension funds, such as investment management. Pension funds should therefore notify the pension supervisory authority if they are considering outsourcing any major functions, and to which parties. If the pension supervisory authority's jurisdiction of powers does not extended to the industries of which the service providers are part, they should oversee these systems indirectly, i.e. via ensuring the pension funds themselves are

[16] See *OECD/ IOPS Guidelines on the Licensing of Pension Entities*
http://www.oecd.org/dataoecd/7/34/40434531.pdf

[17] See *IOPS Principles of Private Pension Supervision*
http://www.iopsweb.org/dataoecd/59/7/40329249.pdf?contentId=40329250

fulfilling their responsibilities in this regard, and through liaising with their appropriate supervisory counterpart, via MOUs, regular industry updates etc.

8.7 Supervisory reviews should where possible include the right to directly address to and request information from a pension fund's service providers (via prescribed conditions in the contract between the pension fund nad the service provider). Alternatively, the pension supervisory authority should have mechanisms in place for liaising with other financial service authorities in order to do so.

8.8 The pension supervisory authority should ensure that outsourcing decisions are made on a rational and arm's-length basis, ensuring that out-sourcing is done via competitive tendering rather than on a relationship basis.

8.9 When assessing a pension fund which already has outstanding outsourcing agreements, the pension supervisory authority should consider whether the governing board is aware of any shortfall in existing arrangement vs. good practices or supervisory guidance, what steps the fund has taken to ensure that arrangements meet such standards, and whether the risks arising as a result of entering into an outsourcing agreement are appropriately covered in the fund's risk management strategy.

Annotations

It is important that supervisors not only assess the effectiveness of the overall system of risk management systems as part of their on-going oversight, but also evaluate the controls over high-risk areas.

Some pension supervisory authorities may use a self-assessment process, in which the pension fund's management reviews the risk management system and certifies to the supervisor that its controls are adequate. Such certifications could be used as part of a licensing/ registration process. The pension supervisory authority would then check whether the self-assessment of the managing board is accurate as part of their on-going oversight.

For on-going supervision, if the pension supervisory authority is satisfied with the quality of the internal audit department's work, the reports of internal auditors can be used as a primary mechanism for identifying control problems, or for identifying areas of potential risk that the auditors have not recently reviewed.

Other pension supervisory authorities may require periodic external audits of key areas where the supervisor defines the scope.

Pension supervisory authorities may combine one or more of the above techniques with their own on-site reviews of internal controls.

During an on-site review, supervisors may ask for 'dummy trades' to be executed on the systems to see how they operate. The less sure the supervisor is of the reliability of the risk management system, the more tests and investigation will need to be carried out.

Pension fund supervisors, in evaluating risk management systems, may choose to direct special attention to activities or situations that historically have been associated with internal control breakdowns leading to substantial losses. Certain changes in the environment should be the subject of special consideration to

see whether accompanying revisions are needed in the risk management system – such as a changed operating environment; new personnel; new or revamped information systems; new technology etc.

As part of its on-going oversight, supervisors can evaluate the work of the internal audit department through review of its work papers, including the methodology used to identify, measure, monitor and control risk. The less the pension supervisory authority can rely on the internal (or external) audit, the more in-depth its own investigation will have to be.

Supervisors will take note of the external auditors' observations and recommendations regarding the effectiveness of internal controls (both during licensing/ registration and on-going supervision) and determine that management and the board of directors have satisfactorily addressed the concerns and recommendations expressed by the external auditors. The level and nature of control problems found by auditors will be factored into supervisors' evaluation of the effectiveness of the internal controls. In some jurisdictions, if the pension supervisory authority does not have expertise in particular areas to conduct in-depth analysis of the internal control of the governing board, it may engage the services of independent, external experts. The skills of the external experts may strengthen the capabilities of pension supervisory authorities.

Discussions of the risk management system will likely form part of the supervisor's frequent contact and enhanced engagement with the management of a pension fund during off-site analysis. Likewise, physical, on-site inspections should include an assessment of a pension fund's risk management architecture, and indeed may be the only way to confirm the quality of the control systems.

A full assessment of a risk management system will require several stages. First the supervisor needs to understand the system which is in place (via studying manuals, internal audit reports etc.). The supervisor will then need to establish whether the systems actually exist in practice. This could be done via a questionnaire sent to key operational staff (asking for specific details on how certain checks are undertaken, for example). Supervisors are in effect acting as 'super external auditors' – with additional scope and powers to their investigations of normal internal and external checks. For example, their investigation may be universal, seeking to establish and overall picture of the risk management architecture, where as an internal operational audit mayonly focus on one division. Also the conclusions of the supervisor will be directed to the board, and any recommendations will be binding.

When evaluating the management and internal control system of a pension fund or plan (either for licensing purposes or as part of ongoing oversight), the pension supervisory authority may undertake the following:[18]

- a review of the minutes of the meeting of the governing board of the pension fund, and detailed examination of the auditor's and actuary's reports;

- an evaluation of the management's capacity to run the fund, their efficiency, and their ability to acknowledge and correct their management mistakes (especially after management changes);

[18] See IOPS Guidelines for *Supervisory Assessment* for further details

- an audit of selected internal procedures and risk control systems, (including internal audit, reporting, monitoring and IT systems), in order to assess the relevance and robustness of these internal controls and the fund's approach to risk management;

- an examination of the accounting procedures in order to know whether the financial and statistical information periodically sent to the pension supervisory authority is reliable or not, and in compliance with the regulations;

- an examination of the governance structure and governance mechanisms of the pension fund (including the segregation between operational and oversight responsibilities);

- fund oversight of outsourced service providers.

In some jurisdictions the pension supervisory authority licenses the service providers directly. Outsourcing of critical or important functions by pension funds should not be undertaken in such a way as to lead to the impairing of the ability of pension supervisory authorities to monitor the compliance of the pension fund with its obligations.

While the pension supervisory authority does not need to approve outsourcing agreements - prior notification of these agreements and material changes in them provides the authority with an opportunity to raise concerns and discuss.